UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/696,495	10/28/2003	Nadarajah Asokan	915-008.013	5756

4955 7590 12/05/2007
WARE FRESSOLA VAN DER SLUYS & ADOLPHSON, LLP
BRADFORD GREEN, BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

EXAMINER	
LE, CANH	
ART UNIT	PAPER NUMBER
2139	
MAIL DATE	DELIVERY MODE
12/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/696,495	**Applicant(s)** ASOKAN ET AL.	
	Examiner Canh Le	**Art Unit** 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 September 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Claims 1- 26 have been examined and are pending.

Response to Arguments

Applicant's arguments, see pages 2-8, filed 09/27/2007, with respect to the rejection(s) of claim(s) 1, 9, 18, and 25 under and 103 (a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Okimoto et al. (US 6,978,022 B2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-4, 6, 8, 9, 11-12, 14, 17-18, 19-23, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Mauro** (US 2002/0147920) in view of **Craft** et al. (US 2002/0150243) ,and further in view of **Okimoto** et al. (US 6,978,022 B2).

As per Claim 1:

retrieving in a secure processing point separated from and arranged in communication with the personal device, a unique chip identifier from a read-only storage of an integrated circuit chip included in the personal device **[par. [0038]); A read only memory (ROM 252) stores secure parameters (e.g., a unique chip identifier) via a secure operation (e.g., during the manufacturing phase) and become available for use thereafter (e.g. retrieving a unique chip identifier)].**

the secure processing point storing a data package in the personal device, the data package including at least one cryptographic key [par. [0034], lines 1-7; A secure unit 240 to perform all secure processing and store all "sensitive" data (e.g. cryptographic key) by various cryptographic technique]

Mauro does not disclose:

receiving at the secure processing point, in response to storing the data package, associating the unique chip identifier with the received backup data package from the personal device, and storing the backup data package and the associated unique chip identifier.

However, Craft et al. disclose:

receiving at the secure processing point, in response to storing the data package, a backup data package from the personal device, which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage of the chip **[par. [0021] and par. [0019]; A server system receives encrypted content data using permanent, hardware-embedded, cryptographic keys (tamper-resistant secret storage) from a client.]**

associating the unique chip identifier with the received backup data package **[par. [0041], lines 7-13; "The manufacture of the client CPU chips also has knowledge of a server public key that is associated with a server private key that may or may not be known to the manufacturer"];**

storing the backup data package and the associated unique chip identifier in a permanent public database **[par. [0043], lines 1-6 and figure 2; A client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database].**

Although the combination of Mauro and Craft teaches the claimed subject matter, they are not so clear of disclosing the secure processing point being separated from the personal device. On the hand, Okimoto teaches this limitation in Column (Col. 5, lines 52-53 of Okimoto).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Mauro by including other feature such as receiving in response to storing the data package, associating the unique chip identifier with the received backup data package, and storing the backup data package and the associated unique chip identifier of Craft and secure processing point being separated from personal device of Okimoto because it would ensure security of the communication between client devices and servers **[par. [0013], lines 1-4, Craft et al]** and securely delivering encrypted content on demand with access control **[Col. 3, lines 67 to Col. 4, line 1, Okimoto].**

As per Claim 25:

Claim 25 is essentially the same as claim 1 except that it sets forth the claimed invention as an apparatus further comprising a processor **[Mauro, fig. 3; box 250, box 230]** rather a method and rejected under the same reasons as applied above.

As per Claim 3:

The combination of teaching Mauro, Craft, and Okimoto teach the claimed subject matter.

Craft et al. further disclose wherein the at least one cryptographic key includes at least one key to be used for a secure, key based communication channel between a personal device manufacturer and the personal device **[par. [0038], figure 2; "a data processing system for secure communication of application code and content using permanent, hardware-embedded, cryptographic key"].**

As per Claim 4:

The combination of teaching Mauro, Craft, and Okimoto teach the claimed subject matter.

Craft et al. further disclose the method as claimed in claim 3, wherein the at least one key to be used for a secure, key based communication channel includes a symmetric key **[par. [0038], lines 1-5; par. [0060], lines 20-24. The symmetric key is a cryptographic key which uses trivially cryptographic key for both decryption and encryption].**

As per Claim 6:

The combination of teaching Mauro, Craft, and Okimoto teach the claimed subject matter.

Craft et al. disclose the method as claimed in claim 3, wherein the at least one key to be used for a secure, key based communication channel includes a private/public key pair **[par. [0038], par. [0032], "Public key cryptography requires each party involved in a communication or transaction to have a pair of key, called the public key and the private key"].**

As per Claim 9:

Mauro discloses a system for managing cryptographic keys that are specific to a personal device, comprising:

at least one personal device **[fig. 1, box 110a; fig. 2]** and a secure processing point **[fig. 2, box 240]**, which secure processing point is separated from and arranged in communication with the personal device,

wherein the at least one personal device includes an integrated circuit chip with a unique chip identifier in a read-only storage and a unique secret chip key in a tamper-resistant secret storage **[par. [0038], lines 1-4. A read only memory (ROM 252) stores secure parameters (e.g., a unique chip identifier); par. [0039], lines 9-11; " secure processor 250 and memory 254 are implemented as two separate units enclosed within a secure and/or tamper resistance/evident unit];**

wherein the secure processing point includes a processor configured for retrieving the unique chip identifier and for storing a data package in the device, the data package including at least one cryptographic key **[par. [0038]; par. [0034], lines 1-7; A secure unit 240 to perform all secure processing and store all "sensitive" data (e.g. cryptographic key) by various cryptographic technique];**

wherein the at least one personal the device includes a processor configured for encrypting the received data package with the unique secret chip key and transferring a resulting backup data package back to the secure processing point **[par. [0036], lines 8-11; "secure processor 250 retrieves data stored within memory 254, processor and/or encrypts the retrieved data, and may send the data to external elements (e.g., main processor 230 via bus 262)];**

Mauro does not explicitly disclose the processor of the secure processing point is arranged for storing the received backup data package.

However, Craft et al. disclose the processor of the secure processing point is arranged for storing the received backup data package in association with the unique chip identifier in a permanent public database **[par. [0043], lines 1-6 and figure 2. A client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database].**

Although the combination of Mauro and Craft teaches the claimed subject matter, they are not so clear of disclosing the secure processing point being separated from the personal device. On the hand, Okimoto teaches this limitation in Column (Col. 5, lines 52-53 of Okimoto).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Mauro by including the processor of the secure processing point is arranged for storing the received backup data package of Craft because it would ensure security of the communication between client devices and servers **[par. [0013], lines 1-4, Craft et al.]** and secure processing point being separated from personal device of Okimoto because it would ensure security of the communication between client devices and servers **[par. [0013], lines 1-4, Craft et al]** and securely delivering encrypted content on demand with access control **[Col. 3, lines 67 to Col. 4, line 1, Okimoto].**

As per Claim 11:

Claim 11 is essentially the same as claim 3 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

As per Claim 12:

Claim 12 is essentially the same as claim 4 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

As per Claim 14:

Claim 14 is essentially the same as claim 6 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

As per Claim 17:

Mauro, Craft, and Okimoto disclose a method as described in claim 1.

Mauro further discloses a method of recovering a backup data package of a personal device, which backup data package has been assembled and stored in accordance with claim 1, the method comprising:

reading a unique chip identifier from a read-only storage of the personal device **[par. [0038]); A read only memory (ROM 252) stores secure parameters (e.g., a unique chip identifier) via a secure operation (e.g., during the manufacturing phase) and become available for use thereafter (e.g. retrieving a unique chip identifier)]**;

Craft further discloses:

transmitting the chip identifier to a public database **[par. [0043], lines 1-6 and figure 2; A client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database].**

receiving from the public database the backup data package corresponding to the transmitted chip identifier **[par. [0015]; lines 8-15; "The client forms a request message, which includes the client serial number, encrypt the request with the**

server public key ad send the download request to the server... the client private key embedded in the client"]; and

storing the received backup data package in the personal device **[par. [0015]; lines 11-15; "The client serial number in the received request is used to search for client public key that corresponds to the client private key embedded in the client"].**

As per Claim 18:

Mauro discloses a personal device comprising:

an integrated circuit chip with a unique chip identifier in a read-only storage and a unique secret chip key in a tamper-resistant secret storage **[par. [0038], lines 1-4. A read only memory (ROM 252) stores secure parameters (e.g., a unique chip identifier); par. [0039], lines 9-11; "secure processor 250 and memory 254 are implemented as two separate units enclosed within a secure and/or tamper resistance/evident unit];**

a memory for storing a received data package including at least one cryptographic key **[par. [0037], lines 1-3. A flash memory is a form of non-volatile memory which is equivalent to memory (130); par. [0034], lines 1-7. A secure unit 240 to perform all secure processing and store all "sensitive" data (e.g. cryptographic key) by various cryptographic technique].**

Mauro does not explicitly disclose:

"a processor configured for outputting the unique chip identifier";

"where the processor is further configured for encrypting the received data package with the unique secret chip key and outputting a resulting backup data package to a permanent public database separated from said personal device". However, Craft et al. disclose:

a processor configured for outputting the unique chip identifier **[par. [0041], lines 7-9; "each CPU chip is assigned a unique client serial number].**

wherein the processor is further configured for encrypting the received data package with the unique secret chip key and outputting a resulting backup data package to a permanent public database separated from said personal device **[abstract , par. [0043], lines 1-6 and figure 2. Encrypting a request which includes a client serial number (216) is equivalent to encrypt the received data package with the unique secret chip key. The client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database].**

Although the combination of Mauro and Craft teaches the claimed subject matter, they are not so clear of disclosing the secure processing point being separated from the personal device. On the hand, Okimoto teaches this limitation in Column (Col. 5, lines 52-53 of Okimoto).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the device of Mauro by including a step of Craft because it would ensure security of the communication between client devices and servers **[par. [0013], lines 1-4, Craft et al.]** and secure processing point being separated from personal device of Okimoto because it would ensure security of the communication between client devices and servers **[par. [0013], lines 1-4, Craft et al]** and securely delivering encrypted content on demand with access control **[Col. 3, lines 67 to Col. 4, line 1, Okimoto].**

As per claim 19:

The combination of teaching Mauro, Craft, and Okimoto teach the claimed subject matter.

Mauro further discloses the personal device as claimed in claim 18, wherein the personal device includes a read-only memory storing a manufacturer public signature key, wherein the memory for storing the received data package is further for storing a received certificate, which corresponds to a certificate stored in association with the backup data package in the public database and which has been signed with a manufacturer private signature key corresponding to the manufacturer public signature key **[par. [0077]; "The signature generation can be performed based on any one of the digital signature and encryption algorithms. Secure processor 250 may further provide the certificate that includes the remote terminal's public key"].**

As per Claim 20:

Claim 20 is essentially the same as claim 3 except that it sets forth the claimed invention as a personal device rather a method and rejected under the same reasons as applied above.

As per Claim 21:

Claim 21 is essentially the same as claim 4 except that it sets forth the claimed invention as a personal device rather a method and rejected under the same reasons as applied above.

As per Claim 22:

Claim 22 is essentially the same as claim 5 except that it sets forth the claimed invention as a personal device rather a method and rejected under the same reasons as applied above.

As per Claim 23:

Claim 23 is essentially the same as claim 6 except that it sets forth the claimed invention as a personal device rather a method and rejected under the same reasons as applied above.

As per Claim 25:

Claim 25 is essentially the same as claim 1 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

Claims 2, 5, 8, 10, 13, 16, 24, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable **Mauro** (US 2002/0147920) , **Craft** et al. (US 2002/0150243) and **Okimoto** et al. (US 6,978,022 B2) as applied to claims **1, 9, 18, and 25** above and further in view of **Messerges** et al. (US 2002/0157002).

As per Claim 2:

Mauro, Craft, and Okimoto disclose the method as described in claim 1 above.

Craft further discloses the secure processing point performs:

associating a unique device identity with the unique chip identifier **[par. [0015]; par. [0041]; client device is equivalent to unique device identity; CPU chip is equivalent to unique chip identifier];**

signing the result of said associating with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the device, thereby generating a certificate for the unique device identity **[par. [0036]; "a data can be signed by computing a digital signature from the data and the private key of signer"];**

storing the unique device identity and the certificate in association with the backup data package and the unique chip identifier in the permanent public database **[par. [0043], lines 1-6 and figure 2; A client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database]**.

Mauro, Craft, and Okimoto do not explicitly disclose storing the certificate in the device;

However, Messerges et al. disclose storing the certificate in the device **[par. [0033]; "The certificate authority is preferably an off-line system, thus every time content is rendered it is not necessary to contact the certificate authority"].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the teachings of Mauro, Craft, and Okimoto by including the step as suggested by Messerges because it would provide a security requirements of digital content while also providing an enjoyable user experience for the end user **[Messerges, par. [0013]].**

<u>As per Claim 26:</u>

Claim 26 is essentially the same as claim 2 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

<u>As per Claim 5:</u>

Mauro, Craft, and Okimoto disclose the method as described in claim 4 above.

Mauro, Craft, and Okimoto do not explicitly disclose "a symmetric key is generated as a function of a master key and the unique device identity".

However, Messerges et al. disclose wherein the symmetric key is generated as a function of a master key and the unique device identity **[par. [0041], lines 36-39; par. [0030]; par. [0068], lines 8-10; par. [0041], lines 36-39. A device manufacturer may be securely embedded keys into a user device so that each user device can be uniquely identified to the other. A unique, factory installed, unit public-key of a user device is equivalent to master key and unique device identity].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the teachings of Mauro and Craft by including the step as suggested by Messerges because it would provide a security requirements of digital content while also providing an enjoyable user experience for the end user **[Messerges, par. [0013]].**

As per Claim 8:

The combination of teaching Mauro, Craft, and Okimoto teach the claimed subject matter.

Craft et al. further disclose the method as claimed in claim 2, wherein the personal device is a wireless communications terminal and the unique device identity is an identifier which identifies the wireless communications terminal in a wireless communications network **[par. [0025], lines 13-16. Personal digital assistant (PDAs, client 107) is equivalent to a wireless personal device].**

As per Claim 10:

Claim 10 is essentially the same as claim 2 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

As per Claim 13:

Claim 13 is essentially the same as claim 5 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

As per Claim 16:

Claim 16 is essentially the same as claim 8 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

As per Claim 24:

Claim 24 is essentially the same as claim 8 except that it sets forth the claimed invention as a personal device rather a method and rejected under the same reasons as applied above.

Claims 7 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable **Mauro** (US 2002/0147920) and **Craft et al**. (US 2002/0150243), and **Okimoto** et al. (US

6,978,022 B2) as applied to claims 1 and 9 above in view of **Ginter** et al. (US patent 5,892,900).

<u>As per Claim 7:</u>

The combination of teaching Mauro, Craft, and Okimoto teach the claimed subject matter.

Craft further discloses generated by the secure processing point during assembly of the device **[par. [0042], lines 1-6. Each client CPU chip has a cryptographic unit (public/private key) that has been manufactured to contain programmable memory storage].**

Mauro, Craft, and Okimoto do not explicitly disclose, "the private/public key pair is generated and store in advance in a secure database before assembly of the device, in which latter case the cryptographic keys stored in advance of assembly are removed from the secret database after reception of the backup data package".

However, Ginter discloses how to generate and store in advance in a secure database before assembly of the device, in which latter case the cryptographic keys stored in advance of assembly are removed from the secret database after reception of the backup data package **[Col. 169, lines 9-17; claim 101. An electronic appliance 600 updates its secure database 610 and/or SPU 500. If an information is received, an end user's electronic appliance 600 requesting the electronic appliance to delete the information that has been transferred. The information comprises at least one or more cryptographic keys]**.

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the teaching of Mauro, Craft, and Okimoto by including how to store the cryptographic keys in advance and removed from the secret database as suggested by Ginter because it would allow the secure database 610 item is updated or modified, a new encryption key can be generated for updated item **[Ginter, Col. 171, lines 43-46].**

As per Claim 15:

Claim 15 is essentially the same as claim 7 except that it sets forth the claimed invention as an apparatus rather a method and rejected under the same reasons as applied above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le

December 03, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100